Whistler Design Preview
April 20 & 21

WMI Enterprise Event Log & Distributed Health Monitoring

Simon Muzio
WMI
Microsoft Corporation

Enterprise Event Log

- What is Enterprise Event Log?
- Scenarios
- Requirements
- Architecture
- Distributed Health Monitoring

What is Enterprise Event Log?

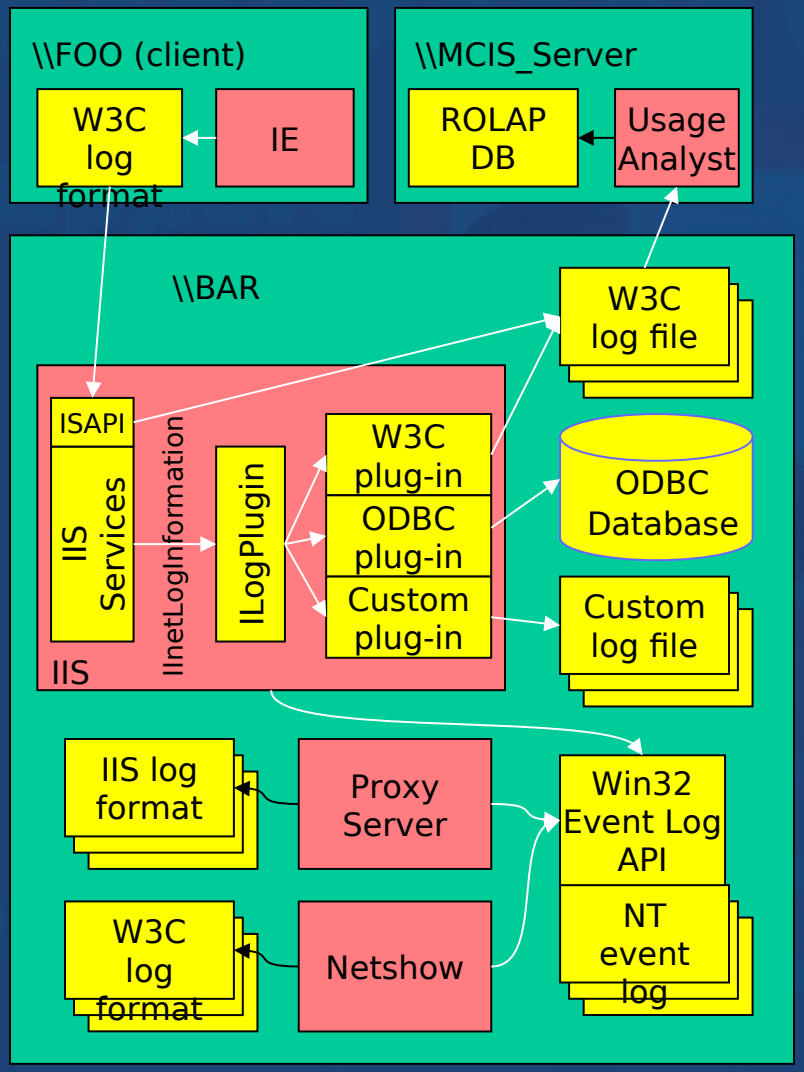
- WMI enterprise-wide logging service for storing events from:
  - Systems (client & server)
  - Applications
  - Network devices
- Policy-based collection events, routing, storing, processing
- Platform for building applications such as billing, auditing, SLA provisioning, health monitoring, web site analysis, performance analysis, capacity planning, and enterprise management,…

What Enterprise Event Log is not

- Not a new event system — EEL uses WMI Events
- Not a new messaging system — EEL uses existing messaging (DCOM & MSMQ)
- Not a new Policy system — EEL uses WMI Policy Based Config which use GPOs.
- Not a new storage system – EEL uses MSDE & Jet

- Not a billing system
- Not a web site analysis system
- Not a performance analysis system
- Not a capacity planning system
- Not an enterprise management system

Logging without Enterprise Event Log



- Many different UI's, API's and schemas for:
  - log format & attribute list
  - log location & naming
  - log rotation (size,time)
- Many different log *local* stores:
  - NT event file
  - IIS proprietary file
  - Perfmon logs
  - w3c file
  - ODBC unnormalized DB
  - Usage Analyst ROLAP DB
- No standard ability:
  - process/filter events
  - centralized storage
  - correlate events

Scenario 1: SLA provisioning / Health Monitoring

- ISP/ITG needs to ensure quality of service
  - Operations configures all datacenter servers, applications, and network devices to log to a central datacenter log store:
    - health information on regular intervals
    - performance information on regular intervals
    - all system and application error events
  - A SLA Provisioning tool provides reports / analysis to business unit/ITG staff when:
    - SLA agreement was violated
      - health log events stop coming from any system, application, or network device; system was unavailable for more that 1 hour
      - monthly Mail service response time exceeded SLA agreement
    - CPU utilization in the last hour on any machine exceeds the recommended level for a given machine

Scenario 2: Capacity planning

- ISP needs to calculate their cost of providing services
  - Operations configures all datacenter servers, applications, and network devices to log to a central datacenter log store:
    - hardware utilization per application per server
  - Capacity planning tool:
    - analyzes trends in utilization over time
    - projects resource requirements for future growth

Scenario 3: Billing

- ISP bills for dialup and IIS hosting based on resource utilization
  - Operations configures all datacenter servers, applications, and network devices to log to a central datacenter log store:
    - Radius connect, “still connected”, and disconnect events
    - IIS bandwidth utilization by destination IP
    - IIS cpu utilization
  - Billing rating engine
    - infer dial-up session duration from the radius events
    - cost ($) each dial-up session
    - cost ($) monthly iis bandwidth use domestic vs international
    - cost ($) iis cpu use
    - queue calculated costs for monthly folding

Scenario 4: Web site analysis

- Marketers want to understand their web site usage
  - Webmaster configures distributed IIS servers to:
    - aggregate system metrics locally
    - filter out iis hits to “accessory” content
    - log iis hits to “quality” content centrally
    - log all user and content metadata updates centrally *(every day at midnight)*
  - Web site analysis system:
    - infers user and visits from iis hit log events
    - resolves IP address to hostnames, hostnames to org names
    - creates PLATO cubes from log storage
    - provides an Excel UI for navigating through the log data
      - Who is coming to the site, what are they looking at, where do they come from? What is selling, who is buying it, drill down by time, demographics, geography, etc.

Scenario 5: Enterprise management

- Big Blue timeshare company unplugs the mainframe and installs an NT server farm
  - Operations configures all enterprise servers, applications, and network devices to log to a central datacenter log store:
    - hardware utilization per application per server
    - authentication events
  - Log data is:
    - archived to a tape system for long term storage
    - extracted from tapes for security audits
    - sent to hardware vendors for capacity planning analysis

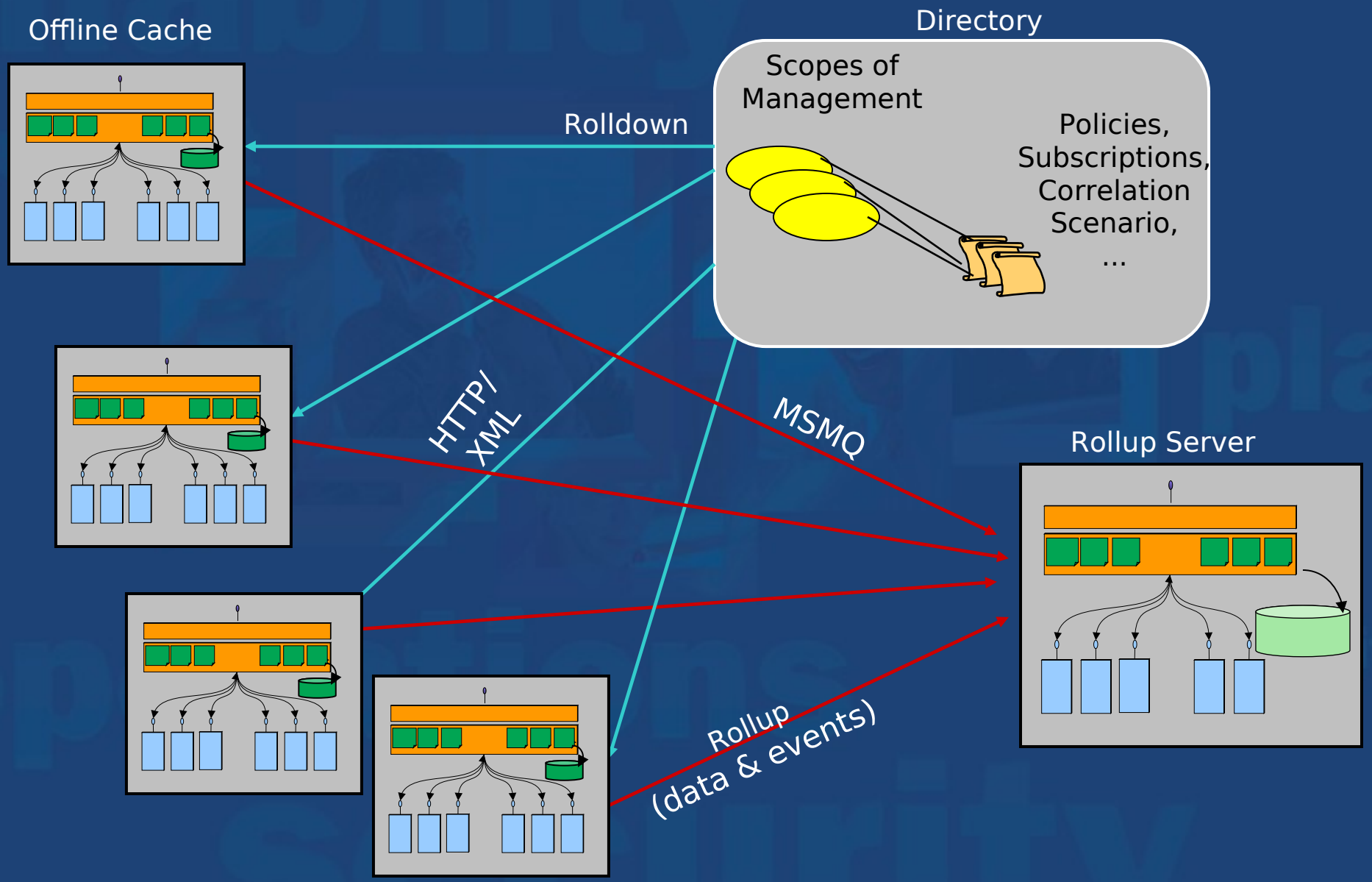
From Scenarios to Requirements

- Enterprise Event Log Administration
  - Define Scope of Management
  - Define & deploy Client-Side Policies
  - Define & deploy Server-side Policies for:
    - Processing events on Rollup server
  - Easy to administer
  - Multi-Admin
- Well-Defined & extensible Log Schema
- Store (local and centralized)
  - Mass Storage repository
  - OLE DB and WMI access to logged events
  - Backup/restore/recovery of mass-storage repository
- Availability / Fault-Tolerance
- Scalable up & out & down
  - Enable multi-tier architecture
  - Physical scalability
  - Slow-link support
- Guaranteed Delivery
- Secure
- Out-of-the box support for centralized rollup/store of existing NT Event Log

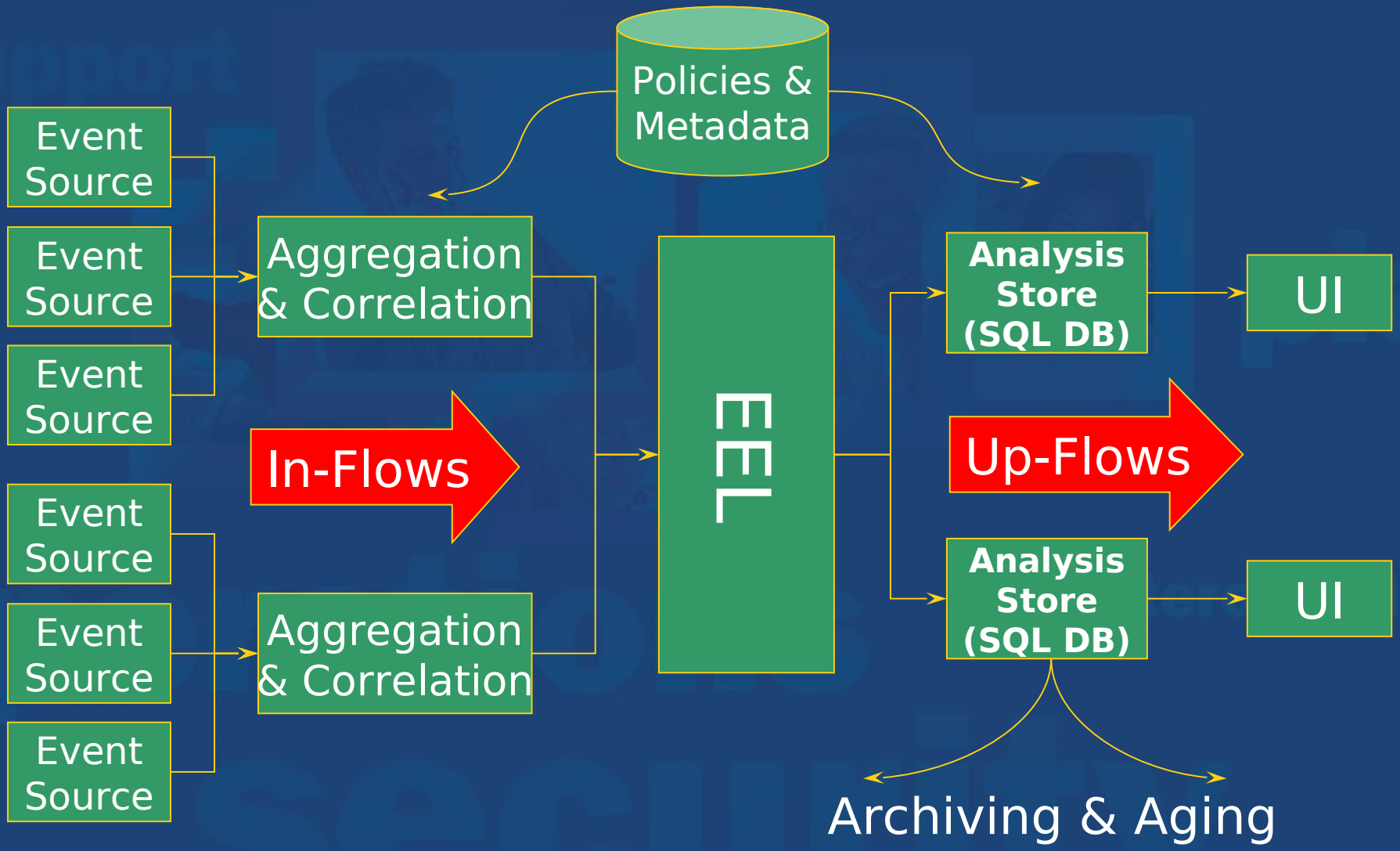
Enterprise Event Log

- What is Enterprise Event Log?
- Scenarios
- Requirements
- Architecture
- Distributed Health Monitoring

WMI Distributed Services



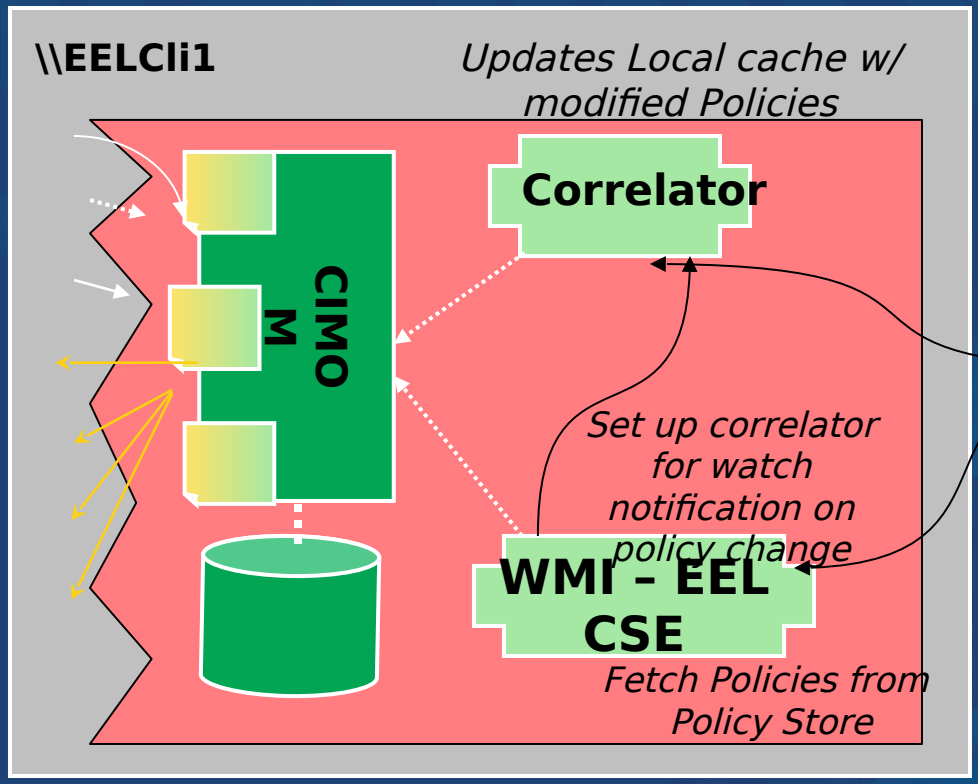
Enterprise Event Log – Logical flows

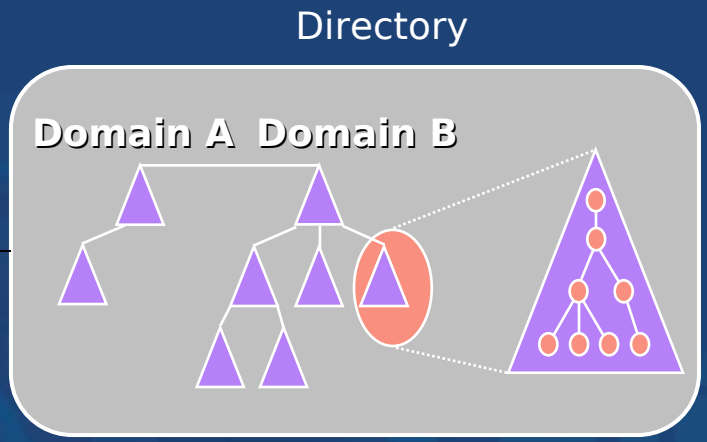


EEL Event Publishing and Collection
Client

- Publish events using WMI
- Collect metrics on specified intervals
- Support NT Event log formats
  - Add WMI Provider for additional formats
- Use WMI Correlator to filter & correlate published events
- Define & act on Quality of Service:
  - High-performance real-time event delivery (in connected env)
  - Guaranteed delivery (disconnected env)
  - Scheduled Up-Load of locally logged events and da

EEL Client Operation





instance of __EventFilter as $F

Query =
"select * from
ExchangeHealthAlert
where Severity < 2";

Filter = $F;
Consumer = $C;
GuaranteedDelivery = true;
QoS = “Single Msg Transaction”;
// Once & Only once
Security = “Auth; Encrypted”;
....
MaxBatchDelay = 3600; // sec
DailySendWindowStart = "1800";
DailySendWindowEnd = "0600";

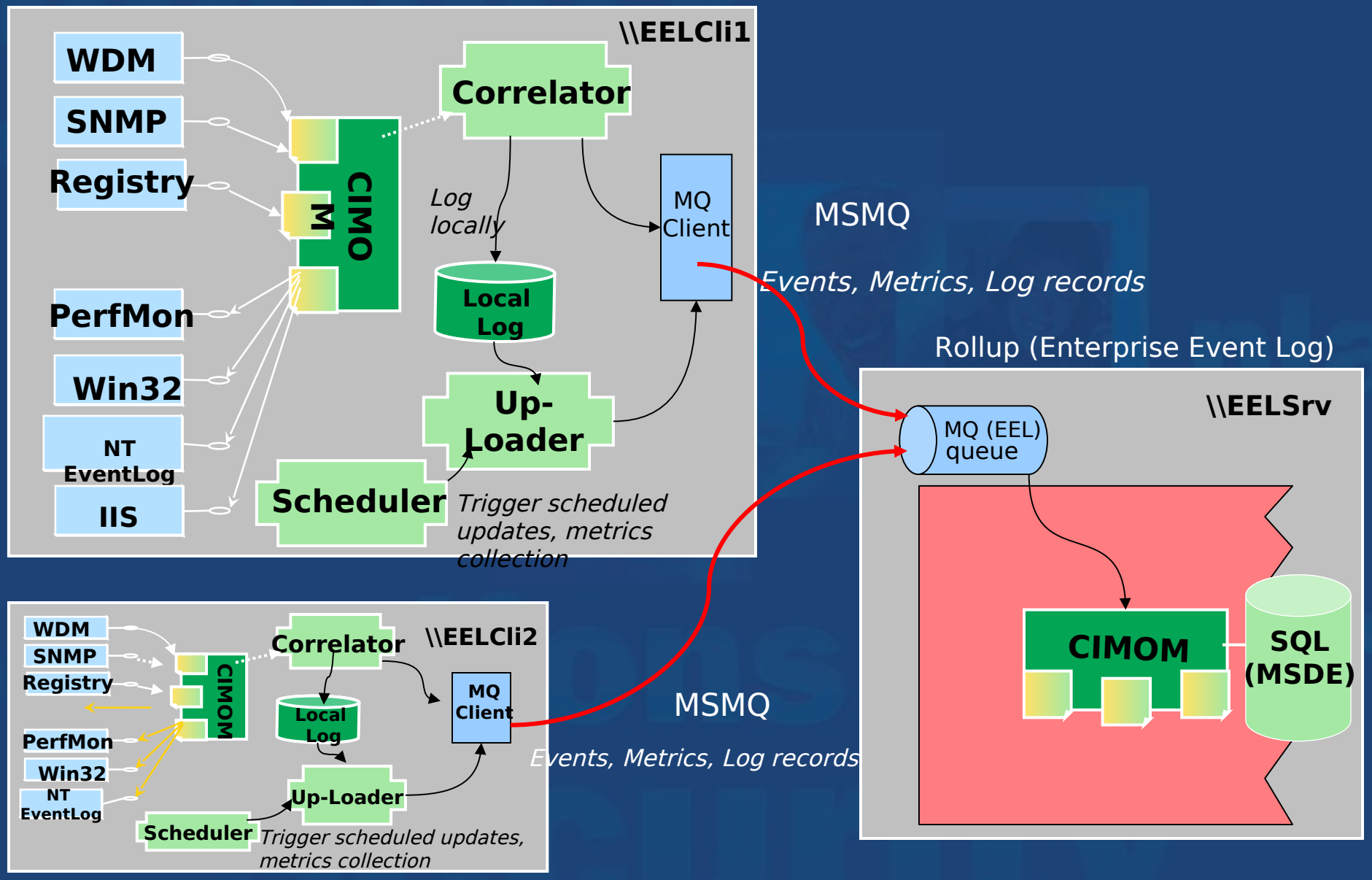
instance of MS_LogToEnterprise as $C

ServerLocation = "myserv1";
LogName = "Exchange";

instance of __FilterToConsumerBinding

Schema
For presentation only

Publishing and Collection



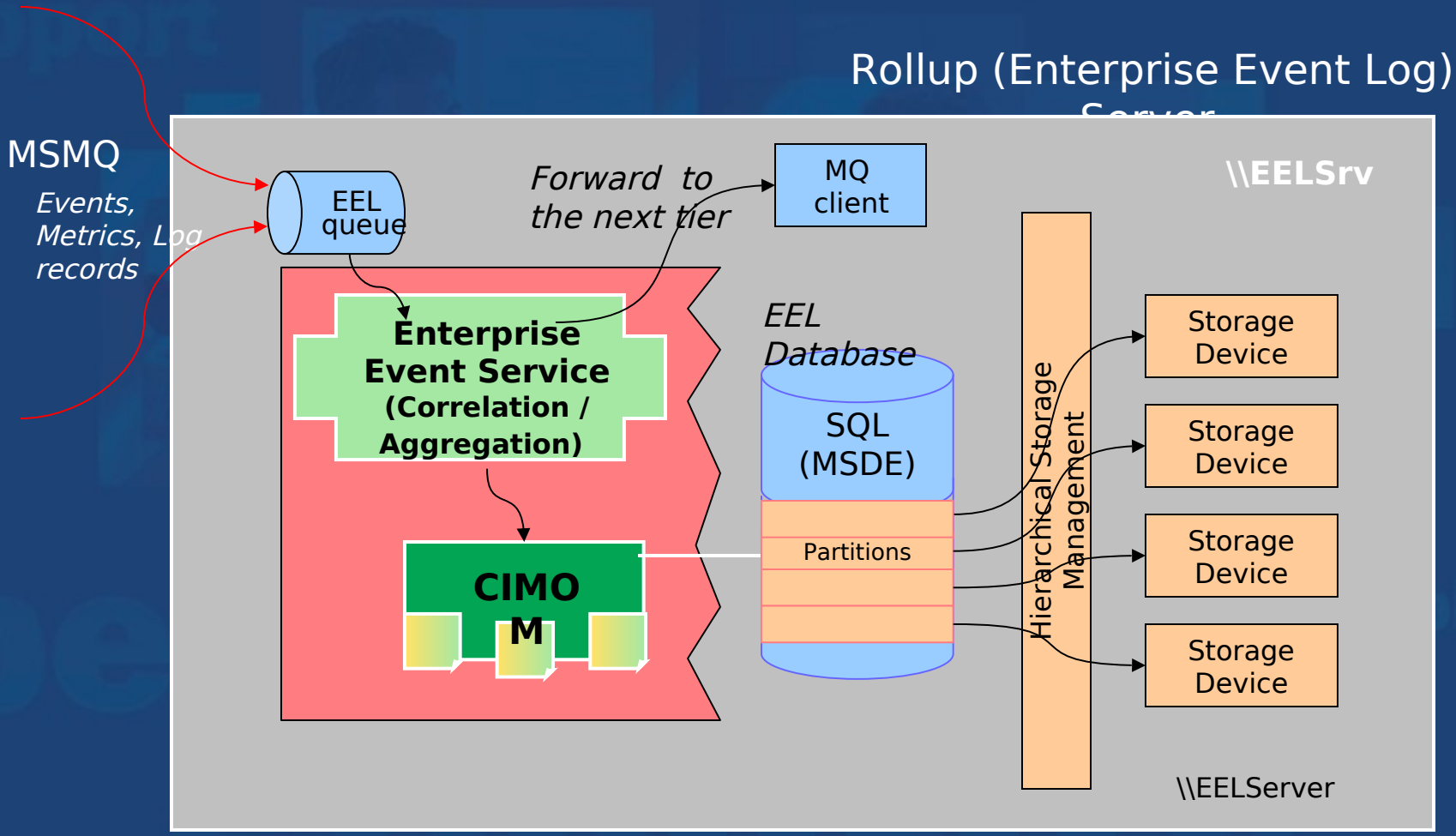
EEL processing
Mid-tier Server

- Correlate/Aggregate events
  - across multiple machines
  - Act on correlator rules results (e.g. do nothing)
- Convert events to Log Records
- Store Log Records in Mass-Storage repository
- Act on Policies/Correlation Rules for Replication/Forwarding to the next tier
- Post-Processing over Stored Data
  - *Can use standard SQL tools*

EEL storage (Mass-Storage support)

- Two stores types with equivalent “write” functionality:
  - MSDE (Rollup server)
  - Local Store (Jet)
- Querieable and Analyzable
  - Optimized for read and random access

Enterprise Event Log Storage



EEL Admin - Policy-based Bootstrap

- Policy Stored in Directory
  - Scopes of Management
  - Meta-Policies (e.g. Refresh)
- Logging Policies:
  - which events (metrics) to log
  - where to log
  - when to send logs (scheduling)
  - how to send: MSMQ (transport) configuration

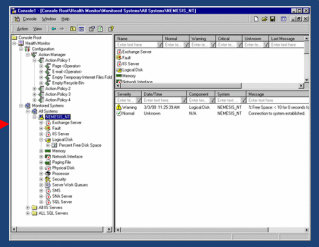
EEL-based Tools

- **EEL viewer**
  - **Will provide EEL and Event Log viewing**
- **EEL Configuration UI**
  - **Configuration of Event forwarding, filtering and logging using EEL Policies**
- **WMI-enabled apps can query directly through WMI**
  - **Discover schema and access data**
  - **Query the DB directly using OLE-DB/ADO**

Logging with Enterprise Event Log

- Applications should just publish events
- Applications have no admin UI for logging
- Scalable to enterprise environment:
  - centralized policy-based management
  - distributed filtering, correlation/aggregation, and storage
- Common Events and Logging Schema
  - enables uniform semantics, built-in processing (correlation/aggregation)
- SQL-based store enables platform for comprehensive analysis
  - cross-machines / end-to-end; over time (historic, ….), trending, root-cause analysis
- Extensible Policy-based system for processing logging events

Distributed Health Monitoring



HealthMon

Forwarder

CIMOM

MSD E

Receiver

To another Tier

MSMQ

Tier1

Forwarder

CIMOM

MSDE

Receiver

Analysis/ Trending

EEL viewer

MSMQ

MSMQ

Forwarder

CIMOM

IIS

Directory

Perf Mon

WDM

NT Event Log

Distributed Health Monitoring

- **Enterprise-wide Health of Network resources**
  - **Provides centralized monitoring**
  - **Applications, machines, components,…**
- **Rollup of Enterprise status using EEL**
- **‘Health’ defined as schema**
  - **Valid ranges of monitored properties defined as WMI schema**
- **Provides problem detection/resolution**
  - **Fix problems as close to the source as possible**
- **Healthmon UI**
  - **Setup, configuration and monitoring**

Additional Resources

- WMI related articles at
- http://msdn.microsoft.com/downloads/sdks/wmi/whitepapers.asp
- http://www.microsoft.com/hwdev/management
- Email wmiinfo@microsoft.com
- Usenet Newsgroup
  - microsoft.public.wbem
- "Managing Windows with WMI" article
  - http://msdn.microsoft.com/library/techart/mngwmi.htm
- "Common Information Model: **Implementing the Object Model for Enterprise Management"**
  - (ISBN 0471253480)


Where do you want to go today?®
Microsoft